Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Юридический институт
Магистратура

УДК 343.98

Новоселова Яна Александровна

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на соискание степени магистра
по направлению подготовки
40.04.01 – «Юриспруденция»

Руководитель ВКР:
к.ю.н., доцент
_____ И.С. Фоминых
«___» _____ 2018 г.

Автор работы:
_____ Я.А. Новоселова

Томск – 2018

Аннотация

магистерской диссертации

на тему: «Криминалистическая характеристика преступлений в сфере компьютерной информации»

В рамках данной работы изучено понятие преступлений в сфере компьютерной информации, рассмотрены основные элементы его криминалистической характеристики, изучена организация его расследования и тактика производства отдельных следственных действий, а также актуальные проблемы выявления и раскрытия преступлений рассматриваемой категории.

Предметом исследования выступают закономерности организации расследования мошенничества с использованием пластиковых банковских карт, а также деятельность органа предварительного следствия и дознания, складывающиеся в сфере выявления, раскрытия и расследования данного вида преступной деятельности.

Объектом исследования стала практика расследования и предупреждения мошенничества с использованием пластиковых банковских карт, научная и учебная литература.

Целью данной работы является комплексная криминалистическая характеристика преступлений в сфере компьютерной информации, их классификация; изучение организации расследования преступлений данной категории; рассмотрение некоторых современных проблем борьбы с киберпреступностью.

Для достижения поставленных в настоящей работе целей и задач применялись общенаучные и частно-научные методы познания.

Структурно работа представлена введением, четырьмя главами, заключением, списком использованных источников и литературы.

Введение содержит формулировки о целях исследования в рамках выбранной темы работы, актуальности этой темы; определяются объект и предмет исследования.

Глава первая – «Преступления в сфере компьютерной информации: общие понятия, криминалистическая классификация». В этой главе рассматриваются общие понятия исследуемой категории, анализируются виды киберпреступлений.

Глава вторая – «Основные элементы криминалистической характеристики преступлений в сфере компьютерной информации» посвящена исследованию способов и обстановки совершения киберпреступлений, изучению личности киберпреступника.

Глава третья – «Использование криминалистической характеристики при расследовании преступлений в сфере компьютерной информации» посвящена изучению типичных следственных ситуаций на первоначальном этапе расследования, тактике производства отдельных следственных действий при расследовании киберпреступлений.

Глава четвертая – «Актуальные проблемы выявления и раскрытия преступлений в сфере компьютерной информации» посвящена существенных проблем предупреждения рассматриваемых преступлений.

В заключении содержатся обобщенные выводы по поводу проведенных исследований в рамках каждой главы.

В работе приводятся примеры из практики, а также мнения исследователей в области криминалистики.

Объем работы составляет 61 страница. Общее количество источников и литературы – 83.

Автор работы  Я.А. Новоселова

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В 1979 году на территории СССР в городе Вильнюс (Литовская ССР) было впервые зарегистрировано преступление, совершенное с использованием компьютера. Факт данного преступления был занесен в международный реестр правонарушений подобного рода и явился моментом возникновения и развития нового вида преступности в России. Другое преступление было совершено в г. Горький. В тот период все отделения связи постепенно переводились на электронный комплекс «Онега», которые обеспечивал обработку принятых и оплаченных денежных переводов. При этом одновременно использовался и обычный прием переводов. Группа нечестных работников воспользовалась наличием автоматизированного и неавтоматизированного приема переводов и совершило хищение. В 1991 г. было раскрыто преступление о хищении 125 000 долларов США во Внешэкономбанке СССР. Как показало расследование, что путем модификации расчетного алгоритма из-под учета электронно-вычислительной машины (далее – ЭВМ) были выведены и подготовлены к хищению еще 750 000 долларов США[1].

С тех пор количество преступлений в сфере компьютерной только возрастало. В 2017 году в России было зарегистрировано 90587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, из них раскрыто - 20424[2].

Без сомнений можно утверждать, что в настоящее время киберпреступность является серьезной глобальной проблемой. Об этом свидетельствуют договоры, принимаемые международным сообществом, для борьбы с данным видом высокотехнологичных преступлений.

---

[1] Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015.С. 45.

[2] Состояние преступности январь - декабрь 2017 года [Электронный ресурс] // Электрон. дан. – 2018. – URL: https://мвд.рф/reports/2/ (дата обращения: 11.02.2018).

Компьютерная преступность зародилась вследствие активного развития компьютерных и информационных технологий. Их совершенствование приводит к росту компьютерной преступности. Следует отметить, что быстрое развитие подобного рода технологий также ведет к качественному изменению киберпреступлений.

Составление исследователями и правоведами теоретических основ и разработка методов борьбы с компьютерными преступлениями всегда на шаг позади стремительно растущих масштабов деятельности преступников. Как результат – высокая латентность компьютерных преступлений [3].

Преступники становятся более изобретательными и используют новейшие технические решения и модифицированное и программное обеспечение. По другую же сторону, техническое и программное обеспечение правоохранительных органов, расследующих киберпреступления, не совершенствуется годами, что приводит к сложностям при расследовании. Все это, в совокупности, подчеркивает **актуальность исследования** в рамках данной выпускной работы.

Выбор темы выпускной работы обусловлен интересом к проблемам расследования киберпреступлений (преступлений в сфере компьютерной информации) и направлен на решение профессиональных задач в будущей профессии.

Термины «преступления в сфере компьютерной информации» употребляются наряду с терминами «киберпреступления» и «компьютерные преступления», их часто используют как синонимы. Наличие различных подходов к определению данных понятий вызывает множество дискуссий.

Целью данной выпускной работы является криминалистическая характеристика преступлений в сфере компьютерной информации, их классификация; изучение организации расследования преступлений данной

[3] Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. 2012. № 24. С. 43 – 46.

категории; рассмотрение некоторых современных проблем борьбы с киберпреступностью.

Для достижения данной цели, необходимо решить определенные **задачи**:

во-первых, провести анализ различных подходов к определению понятия «преступления в сфере компьютерной информации», соотнести с понятиями «компьютерные преступления» и «киберпреступления»;

во-вторых, изучить классификации преступлений в сфере компьютерной информации;

в-третьих, рассмотреть основные элементы криминалистической характеристики преступлений в сфере компьютерной информации, такие как способ и обстановка совершения преступления;

в-четвертых, изучить личность киберпреступника;

в-пятых, изучить организационные основы расследования киберпреступлений;

и, наконец, в-шестых, дать общую характеристику актуальных проблем расследования компьютерных преступлений.

Предметом исследования выступают закономерности организации расследования мошенничества с использованием пластиковых банковских карт, а также деятельность органа предварительного следствия и дознания, складывающиеся в сфере выявления, раскрытия и расследования данного вида преступной деятельности.

Объектом исследования стала практика расследования и предупреждения мошенничества с использованием пластиковых банковских карт, научная и учебная литература.

Методологическую основу диссертационного исследования составляет совокупность общих и частных методов научного познания.

Теоретическую базу проведенных исследований составляют труды отечественных и зарубежных ученых, таких как, В.Б. Вехов, Т.Л. Тропина, Н.Н. Федотов, Е.С. Шевченко и других.

Эмпирическую базу исследования составляют следующие источники:

- материалы уголовных дел, связанных с преступлениями в сфере компьютерной информации, расследованных на территории различных субъектов Российской Федерации;

- следственная практика и статистические данные, а также результаты эмпирических обобщений, проведенных другими исследователями.

Научная новизна диссертационного исследования заключается в рассмотрении современного этапа развития набирающей все большую актуальность проблемы, затрагивающей вопросы криминалистического обеспечения расследования преступлений в сфере компьютерной информации.

Структура магистерской диссертации обусловлена поставленными целями и задачами, объектом и предметом исследования. Диссертация содержит введение, 4 главы, заключение, список использованных источников и литературы.

ГЛАВА 1 Преступления в сфере компьютерной информации: общие понятия, криминалистическая классификация

1.1 Определение понятия «преступления в сфере компьютерной информации»

Глобальные процессы, происходящие в политике, экономике, науке и технике оказали существенное влияние на все сферы жизни современного общества и отдельного человека в нём, привели к серьёзным изменениям или возникновению абсолютно новых феноменов. На пороге XXI века быстрыми темпами развиваются компьютерные технологии. Однако все эти достижения имеют свою «оборотную» сторону, а именно - компьютерную преступность.

Весь спектр преступных действий в сфере информационных технологий, будь то преступления, которые совершенны при помощи компьютеров, или те, предметом которых стали сами компьютеры, компьютерные сети и хранящаяся в них информация охватываются понятием «интернет-преступление» или «киберпреступление». «Компьютерное преступление» – это только то преступление, которое посягает на безопасное функционирование компьютеров и компьютерных сетей, а также на обрабатываемые ими данные[4].

В настоящее время мировым сообществом не выработаны единая терминология и подход к определению понятию «преступления в сфере компьютерной информации», которое употребляется наряду с понятиями «компьютерная преступность» и «киберпреступность».

В Уголовном Кодексе содержится состоящая из трех статей (272-274) глава «Преступления в сфере компьютерной информации». В соответствии с примечанием к ст. 272 УК под компьютерной информацией понимаются

[4] Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. 2016. № 1 (35). С. 22.

«сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[5].

То есть под преступлениями в сфере компьютерной информации следует понимать общественно опасные деяния (предусмотренные главой 28 Раздела IX УК РФ), которые посягают на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Термин же «компьютерные преступления» несколько шире, чем «преступления в сфере компьютерной информации». Он охватывает и те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления (понятно, что из разряда компьютерных преступлений мы исключаем такие преступления, в которых компьютерная техника используется лишь как материальная ценность) или объектом посягательства. К таким преступлениям относятся: мошенничество с применением банковских карт (кардинг), мошенничество с выманиванием персональных данных (фишинг), незаконное пользование услугами связи и иной обман в области услуг связи, промышленный и иной шпионаж, когда объектом являются информационные системы, и т.д.

Глобальная сеть нематериальна и не может быть сведена к физическому воплощению. Потому термин «компьютерная преступность» по своему смыслу определяет суть преступлений, совершенных с помощью компьютера. Однако в настоящее время, само понятие «компьютер» в размыто, так как практически все мобильные телефоны имеют доступ во всемирную сеть Интернет. Так, например, развитие LTE (сеть четвертого поколения) позволяет получить доступ к глобальной сети с такой скоростью и качеством, что не только не уступает по возможностям подключению к

[5] Уголовный кодекс РФ [Электронный ресурс]: Федеральный закон от 13.06.1996 № 63-ФЗ принят ГД ФС РФ (с учетом всех поправок от 01.02.2018 г. № 139-ФЗ) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2018. – Доступ из локальной сети Науч. б-ки Том. гос. ун-та. (дата обращения 15.02.2018).

сети Интернет с помощью обычного персонального компьютера, но, порой, и превышает их.

В мировой практике термин "киберпреступность" впервые появился во второй половине XX века. Первые подобные преступления были связаны с проникновением в компьютерные системы путем их повреждения и хищением данных.

С течением времени, и как следствие развития компьютерных и телекоммуникационных технологий, понятие "киберпреступность" изменялось, включая в себя все новые и новые преступления.

Традиционные формы компьютерных преступлений переходили в новые, такие как: компьютерное мошенничество, несанкционированный доступ к личным данным, незаконное использование программного обеспечения[6].

Современные тенденции развития киберпреступности продолжаются и в XXI веке. Общедоступность глобальной сети Интернет, простота в использовании, анонимность и высокая скорость передачи данных превратила локальные киберпреступления в транснациональную киберпреступность.

В зарубежной литературе и во многих официальных документах кроме/вместо «computer crime» также часто употребляется термин «cyber crime» – киберпреступность, киберпреступление. Определения этого термина разные, существуют широкие и узкие трактовки.

Некоторыми исследователями киберпреступность связывается с преступлениями, совершаемыми в различных информационных сетях. Так, по мнению А.В. Суслопарова "термин "киберпреступность" оправдан, если

[6] M. Gercke. Understanding cybercrime: a guide for developing countries. ITU, Geneva 2011 [Электронный ресурс]. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_ Guide_A5_12072011.pdf (дата обращения 19.02.18).

мы говорим о совершении компьютерных преступлений в рамках компьютерной сети, в частности, сети Интернет[7].

С.В. Воронцов отмечает, что "термин "киберпреступность" используется для определения преступности в виртуальном пространстве, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в локальных и глобальных сетях"[8].

В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков считают, что "киберпреступность" – это любое преступление, совершенное с помощью компьютерной сети, т.е. любое преступление, совершенное в электронной среде[9].

И.Г. Чекунов включает в понятие "киберпреступности" компьютерные средства и мобильную (сотовую) технику. По его мнению "под киберпреступностью следует понимать совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных"[10].

Высказана также точка зрения, согласно которой киберпреступность относят к преступлениям, совершаемым посредством компьютерной техники против различных прав и благ человека. Такой позиции придерживается В.А. Номоконов, который определяет киберпреступность как "родовое понятие, охватывающее как компьютерную преступность в узком значении этого слова (где компьютер является предметом, а информационная безопасность – объектом преступления), так и иные посягательства, где компьютеры

---

[7] Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера: дис. … канд. юрид. наук. Красноярск, 2010. С. 24.

[8] Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний // Российская юстиция. 2011. № 2. С. 14 - 15.

[9] Дуленко В.А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учебное пособие. Уфа, 2007. С. 27.

[10] Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. С. 37 - 44.

используются как орудия или средства совершения преступлений против собственности, авторских прав, общественной безопасности или нравственности"[11].

В.А. Номоконов и Т.Л. Тропина обращаются к толковым словарям Оксфордского и Кембриджского университетов, и определяют приставку кибер (cyber) как «относящийся к информационным технологиям, сети Интернет, виртуальной реальности» и «включающий в себя использование компьютеров или относящийся к компьютерам, особенно к сети Интернет»[12].

Стоит отметить, что существует и обобщенный подход. Так, мнению Т.Л. Тропиной, киберпреступность – это «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных».[13]

Международное право двинулось по пути разделения понятий «киберпреступность» и «компьютерные преступления». Советом Европы была принята Конвенция о киберпреступности (ноябрь 2001 г.), в которой был употреблен термин «киберпреступность» («cybercrime»), а не «компьютерные преступления» («computer crime»).

В 2013 году Управлением ООН по наркотикам и преступности был опубликован отчет, в котором было отмечено, что понятие «киберпреступность» зависит от контекста и цели его употребления. В этом же документе отмечается, что в рассматриваемое понятие включаются любые деяния, направленные на нелегальное извлечение прибыли и иная противозаконная деятельность в киберпространстве.

---

[11] Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Компьютерная преступность и кибертерроризм: сборник научных работ. 2004. №. 1. С. 77.

[12] В.А. Номоконов, Л.В. Тропина Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 47.

[13] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно–правовые меры борьбы: автореф. дис. ... канд. юрид. наук. Владивосток, 2005. С. 9.

В связи с вышесказанным мы считаем, что понятие киберпреступности является совокупностью преступлений и распространяется на различные виды преступлений, которые совершаются в информационно-телекоммуникационной сфере, в которой информация, информационные ресурсы и техника могут являться целью преступного посягательства, совершаемого с использованием различных средств.

1.2 Виды преступлений в сфере компьютерной информации

23 ноября 2011 г. в Будапеште была подписана Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185[14]. Она была подписана государствами-членами Совета Европы, а также США и Японией. В настоящий момент Россия не подписала Конвенцию. Тем не менее, Конвенция содержит важные положения и проводит классификацию киберпреступлений, выделяя их виды в 5 групп.

Первая группа: преступления, которые посягают на конфиденциальность, целостность и недоступность компьютерных данных и систем. Примером можно назвать, например: несанкционированный доступ в базы данных и в систему.

Вторая группа: преступления, связанные с использованием компьютера как средства совершения противозаконных действий. К этой группе можно отнести компьютерное мошенничество.

Третья группа: преступления, связанные с содержанием информации, размещаемой в сети Интернет. В частности с размещением в сети детской порнографии.

Четвертая группа: преступления, связанные с нарушением авторского права и смежных прав. Однако установление таких правонарушений

[14] Counsil of Europe. Convention on Cybercrime, Budapest. [Электронный ресурс] // Электрон. дан. – 2017. – URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/ (дата обращения 20.10.17).

Конвенцией отнесено к компетенции национальных законодательств государств.

Пятая группа: преступления, связанные с распространением расистских и ксенофобских материалов в сети Интернет.

Анализируя уголовные дела по преступлениям в сфере компьютерной информации и изучая работы отечественных ученых в сфере киберпреступлений, возможно выделение более 20 основных способов совершения компьютерных преступлений и еще большего числа их разновидностей. Такое количество способов совершения преступлений в рассматриваемой сфере постоянно растет в связи с развитием компьютерной техники, коммуникационных сетей, а также разнообразием модификаций средств (аппаратных и программно-аппаратных) совершения киберпреступлений.

Следующие виды киберпреступлений выделяет Д.А. Илюшин:

1. Неправомерное подключение к сети Интернет;
2. Создание, использование и распространение вредоносных программ;
3. Незаконное изготовление, хранение, распространение, рекламирование и (или) публичная демонстрация информации, запрещённой к свободному обороту, совершённое с использованием сети Интернет;
4. Нарушение авторских и смежных прав, а также незаконное использование чужого товарного знака, совершённые с использованием сети Интернет;
5. Компьютерное мошенничество;
6. Хищение электронных реквизитов и сбыт поддельных кредитных либо расчётных карт;
7. Незаконное предпринимательство в сфере предоставления услуг Интернет;
8. Вымогательство, совершённое с использованием сети Интернет;

9. Кибертерроризм[15].

По предмету преступного посягательства преступления подразделяются на преступления, имеющие материальный предмет посягательства, и преступления, не имеющие такового. По численности субъектов преступления – совершённые одним лицом; группой лиц.

В.А. Мещеряков классифицирует преступления в сфере компьютерной информации по объекту преступного посягательства – компьютерной информаций. На основе этого критерия выделяет следующие виды:

1. Уничтожение (разрушение) компьютерной информации.
2. Неправомерное завладение компьютерной информацией или нарушение исключительного права на её использование:
   - Неправомерное завладение алгоритмом (методом) преобразования компьютерной информации;
   - Неправомерное завладение совокупностью сведений, документов – нарушение исключительного права владения;
   - Неправомерное завладение компьютерной информацией как товаром.
3. Действия или бездействие по созданию компьютерной информации с заданными свойствами:
   - Распространение по телекоммуникационным каналам информационно-вычислительных сетей компьютерной информации, наносящей ущерб абонентам;
   - Разработка и распространение компьютерных вирусов и прочих вредоносных программ для ЭВМ.
4. Неправомерная модификация компьютерной информации:
   - Неправомерная модификация компьютерной информации как совокупности фактов, сведений;

[15] Илюшин, Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: Дис. … канд. юрид. наук / Д.А. Илюшин. Волгоград, 2008. С. 155.

- Неправомерная модификация компьютерной информации как алгоритма;
- Неправомерная модификация компьютерной информации как товара с целью воспользоваться её полезными свойствами[16].

В.Б. Веховым компьютерные преступления следует классифицировать по роли компьютерной техники в механизме преступного деяния:

1) во-первых, когда компьютерная техника выступает в роли предмета посягательства;

2) во-вторых, когда компьютерная техника выступает в роли орудия и средства совершения преступления. В этом случае предметом посягательства является информация, а орудием выступает компьютерная техника[17].

Несмотря на то, что существует множество видов киберпреступлений, все они имеют индивидуальные признаки, позволяющие классифицировать их по способу совершения. На этом основании можно выделить классификацию И.А. Морар:

1. Совершение с помощью компьютерных технологий и соответствующей техники традиционных преступлений, включая преступления, направленные на присвоение либо повреждение этой техники.
2. Нелегальное получение товаров и услуг.
3. Перехват информации.
4. Неправомерный доступ к компьютерной информации и ее хищение:

- посягательство на компьютерную информацию, находящуюся на одном из серверов глобальной компьютерной сети;

- посягательство на информацию, находящуюся в аппаратных средствах.

5. Компьютерное пиратство (нарушение авторских прав).
6. Хищения, связанные с переводом электронной наличности.

---

[16] Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста: научный журнал. 2013. № 5 (10). С. 265 - 270.

[17] Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского – М.: Право и закон, 1996. – С. 27.

7. Компьютерный «терроризм» и «вандализм».

8. Мошенничество в сфере электронной торговли и инвестирования.

9. Электронные способы легализации преступных доходов.

10. Уклонение от налогов.

11. Распространение нелегальных материалов (экстремизм, порнография).

12. Прочие преступления[18].

Отметим и зарубежную классификацию: кодификатор Международной уголовной полиции «Интерпол», который содержится в документе «Руководство Интерпола в компьютерной преступности».

Все киберпреступления, которые в документе обозначаются буквой «Q». Также имеется дополнительный идентификатор для обозначения определенной группы преступлений. Всего выделяется шесть групп:

1. Несанкционированный доступ или перехват (QA).

Неправомерный доступ к компьютерной системе или сети путем нарушения систем охраны.

Несанкционированный перехват – неправомерный и осуществленный с помощью технических средств перехват сообщений, приходящих в компьютерную систему или сеть, исходящих из компьютерной системы или сети и передаваемых в рамках компьютерной системы или сети.

2. Изменение компьютерных данных (QD).

Изменение компьютерных данных – неправомерное изменение данных с использованием вредоносного программного обеспечения.

3. Компьютерное мошенничество (QF).

Компьютерное мошенничество – введение, удаление или изменение компьютерных данных или программ, либо иное вмешательство в процесс обработки данных, с намерением получить незаконным путем

[18] Морар И.О. Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия? // Российский следователь. – 2012. – № 12. – С. 37 – 41.

экономическую выгоду. Может осуществляться с целью хищения и последующего использования данной информации или же ради развлечения.

Существует множество способов осуществления несанкционированного доступа к системе, как правило, с использованием чужого имени; подбором паролей; изменением адресов устройств; использованием информации, оставшейся после решения задач; модификацией программного и информационного обеспечения, использование фишинговых ссылок и т.д.

4. Незаконное копирование – «пиратство» (QR).

Незаконное копирование – «пиратство» – несанкционированное копирование программного обеспечения и иных форм интеллектуальной собственности.

5. Компьютерный саботаж (QS).

Компьютерный саботаж – введение, удаление или изменение компьютерных данных или программ с целью воспрепятствовать нормальному функционированию компьютера или сети.

6. Прочие компьютерные преступления (QZ)[19].

В данную подгруппу внесены такие киберпреступления, как: хищение информации, составляющей коммерческую тайну, передача конфиденциальной информации и прочие.

Формирование теории криминалистической классификации киберпреступлений способствует наиболее правильному выбору тактики и методики расследования киберпреступлений, с практической точки зрения криминалистическая классификация необходима для гарантии всесторонности и полноты расследования. Дальнейшая разработка теоретических основ криминалистической классификации киберпреступлений обусловлена потребностями криминалистической теории

[19] Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М.: Новый Юрист, 1998. – С. 53 – 54.

и практики выявления и расследования преступлений в сфере высоких технологий.

ГЛАВА 2 Основные элементы криминалистической характеристики преступлений в сфере компьютерной информации

2.1 Способ совершения

Уже немало исследований так или иначе затрагивали проблемы способов совершения преступлений против собственности, личности, общественной безопасности и общественного порядка и др., в то время как применительно к компьютерным преступлениям категорию способа совершения преступления достаточно сложно проработать.

В работах криминалистов встречаются различные мнения по вопросу о видах способов совершения компьютерных преступлений. Несмотря на множество различных классификаций способов совершения киберпреступлений. В целом они могут быть разделены на две большие группы.

1) Первая группа – способы с непосредственным воздействием на информацию (путем проникновения в компьютер и введения различных команд);

2) Вторая группа – способы с удаленным воздействием на информацию (путем введения чужих реквизитов идентификации, и использованием вредоносных программ для удаленного доступа и т.д.)

Н.И. Шумилов предлагает разделять способы совершения посягательств на три самостоятельные группы:

• незаконное изъятие носителей информации;

• несанкционированное получение информации;

• неправомерное манипулирование информацией[20].

Представляется, что перечисленные группы отображают многообразие не способов совершения преступления, а самих преступных деяний. Кроме того, к данным группам можно отнести не все, а только некоторые деяния, предусмотренные ст.ст.272-274 УК РФ, следовательно, классификация

[20] Шумилов Н.И. Криминалистические аспекты информационной безопасности: Дис. ... канд. юрид. наук. СПб.: Юр. инст., 1997. С. 22.

является неполной. Внутреннюю противоречивость придает ей и тот факт, что, по нашему мнению, незаконное изъятие носителя информации является не чем иным, как частным случаем несанкционированного ее получения; а неправомерное манипулирование информацией может сводиться, например, к шантажу.

И.О. Морар приводит совершенно иную классификацию компьютерных преступлений, основанную на своеобразии способов их совершения. Он выделяет:

1) способы, применимые для получения доступа к информации, находящейся на машинных носителях (аппаратные устройства компьютерного типа, телефоны, пейджеры, аналоговые записывающие устройства и т.д.);

2) способы, где компьютерная техника и средства коммуникации используются в качестве орудий и средств совершения преступления и/или их сокрытия;

3) способы, где применяются высокотехнологичные устройства с целью незаконного доступа к компьютерной информации, ее модификации или блокирования[21].

Она представляется нам еще более запутанной ввиду того, что первая и третья группа способов являются, по сути, одинаковыми, ведь из текста автора непонятно, чем «простой» доступ к информации отличается от доступа с применением «высокотехнологичных» устройств, и где критерий их «технологичности».

Используя методологический подход Ю.М. Батурина, можно выделить следующие виды способов совершения киберпреступлений:

1) изъятие средств компьютерной техники (далее СКТ);

2) перехват информации;

[21] Морар И.О. Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия? // Российский следователь. 2012. – № 12. – С. 37 – 41.

3) несанкционированный доступ к СКТ;

4) манипуляция данными и управляющими командами;

5) комплексные методы.

Первая группа – наиболее распространенные способы некомпьютерных преступлений, в которых действия преступника направлены на изъятие чужого имущества. Под чужим имуществом в данном случае понимаются средства компьютерной техники, подробно классифицированные нами в первой главе работы.

Отличительная черта рассматриваемой группы способов совершения компьютерных преступлений в том, что средства компьютерной техники будут выступать только в качестве предмета преступного посягательства, а в качестве орудия совершения преступления будут использоваться другие инструменты, технические устройства и приспособления, которые не являющиеся средствами компьютерной техники.

Вторая группа способов совершения компьютерных преступлений - это основанные на действиях преступника, которые направлены на получение данных и информации посредством перехвата.

Третья группа способов совершения компьютерных преступлений – это действия преступника, которые направлены на получение несанкционированного доступа к СКТ.

Четвертая группа – действия преступников, которые связаны с использованием методов манипуляции данными и командами СКТ.

Пятая группа способов – комплексные методы, которые включают в себя различные комбинации рассмотренных способов совершения компьютерных преступлений. По международной классификации в отдельную группу принято выделять такие способы, как компьютерный саботаж с аппаратным или программным обеспечением, которые приводят к выводу из строя компьютерной системы. Наиболее значительные компьютерные преступления совершаются посредством порчи программного

обеспечения, причем часто его совершают работники, недовольные своим служебным положением, отношением с руководством и т.д.

Безусловно, есть и другие точки зрения. Например, В.Б. Вехов не дает развернутой классификации, он лишь определяет ее будущие очертания путем выделения оснований (критериев):

- во-первых, когда компьютерная техника выступает в роли предмета посягательства;

- во-вторых, когда указанная техника выступает в роли орудия и средства совершения преступления[22].

Так или иначе, вопрос о выделении способов совершения преступления требует, в первую очередь, детальной переработки и привлечения экспертов в сфере информационных технологий.

Следует обратиться ко второму аспекту проблемы – использованию компьютерных технологий и компьютерных устройств как самостоятельному способу совершения преступления. Научно-технический прогресс изменяет орудия, средства и способы деятельности. К сожалению, обратной стороной медали является использование всех его достижений в преступных целях.

Так, в последнее время неуклонно растет количество хищений со счетов граждан в банках с использованием заранее похищенных или поддельных расчетных карт, внедрений считывающих модулей и вредоносных программ в банковское оборудование, хищений с электронных (виртуальных) кошельков платежных систем и т.д. Это лишь малая часть преступных действий, совершаемых с применением компьютерных технологий, но та часть, с которой наверняка сталкивались многие граждане.

Необходимо учитывать, что компьютерные преступления – это, с одной стороны, преступления, совершаемые в сфере компьютерной информации и безопасности с применением особых, программных и технологических средств и приемов, но, с другой стороны, большинство

[22] Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского. М.: Право и закон, 1996. С. 34.

преступлений, совершаемых с применением этих средств – это всем хорошо известные преступления (против личности, собственности, общественной безопасности и общественного порядка и т.д.), но совершаемые в особой социально-технологической среде.

Также следует сделать вывод о том, что в преступлениях, способ совершения которых сопряжен с использованием компьютерных технологий, программы и ИТКС должны признаваться средствами совершения преступления, а компьютерное оборудование и устройства – орудиями, со всеми вытекающими из этого последствиями. Способ совершения таких преступлений должен включать как собственные действия преступника, так и действия, осуществляемые при помощи компьютерных программ, что следует учитывать при установлении момента фактического окончания преступных действий.

Подводя итог, следует сказать, что существуют множество видов способов совершения киберпреступлений и различные основания для их выделения, что доказывает сложность создания единой классификации в данной сфере. По причине развития компьютерных технологий приводит к появлению новых способов совершения киберпреступлений. Таким образом, вопрос о способах совершения киберпреступлений является важной составляющей для своевременного выявления, раскрытия и предупреждения рассматриваемых преступлений.

2.2 Обстановка совершения преступления

Изучение обстановки совершения преступления необходимо для криминалистической характеристики киберпреступлений. В настоящее время

данный вопрос в литературе недостаточно разработан и требует дальнейшего изучения и исследования[23].

Обстановка совершения преступлений включает в себя взаимодействующие между собой до и в момент преступления объекты, процессы и явления, характеризующие время, место, вещественные и иные условия окружающей среды, поведение непрямых участников преступления и другие факторы, определяющие возможность, условия и обстоятельства совершения преступления. Обобщенные знания об обстановке преступления, находящейся во взаимосвязи с другими элементами криминалистической характеристики, позволяют акцентировать внимание следствия на более эффективный поиск и установление обстоятельств, входящих в предмет доказывания[24].

Особенностью обстановки преступления является ее динамичность. Преступник всегда оценивает существующую обстановку до и в момент совершения преступления как благоприятную или неблагоприятную, причем не всегда верно [25] . Следствие же, наоборот, при ретроспективной направленности расследования встречается с обстановкой, сложившейся после совершения преступления и зачастую измененной естественными, производственными, случайными и иными факторами. Так, при осмотре места происшествия следователь встречается со следами преступника, затертыми посторонними лицами[26].

Специфика составляющей обстановки совершения киберпреступлений – время и место совершения. Действия происходят в виртуальном

---

[23] Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. … канд. юрид. наук. Барнаул, 2009. С. 112.

[24] Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АГУ. 2013. № 2-1 (78). С. 114 – 116.

[25] Гавло В.К. Обстановка преступления как структурный компонент криминалистической характеристики преступления // Проблемы совершенствования тактики и методики расследования преступлений : сб. науч. трудов. Иркутск, 1980. С. 49 – 55.

[26] Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АГУ. 2013. № 2-1 (78). С. 114 – 116.

пространстве и использованием телекоммуникационных сетей, причем одновременно злоумышленником могут быть задействовано несколько компьютеров, находящихся в разных местах (порой в разных государствах)[27]. Каждое из таких мест имеет свою обстановку.

Следует отметить, что преступник действует не только в конкретной обстановке, но и в конкретное время, порой в значительной мере влияющее на его поведение. Работа некоторых программ связана со временем, установленным на компьютере, которое может быть изменено по желанию преступника. Установление точного времени совершения преступления является сложной задачей, разрешение которой не всегда возможно.

Обстановка сильно влияет на киберпреступников. Как показывает практика, в большинстве случаев проводится основательная подготовка к совершению преступления[28]. Проводится сбор и изучение необходимой информации, имеющихся технологиях, в частности о средствах защиты и их характеристиках. Задачей злоумышленника становится адаптация и внедрение в коммуникационные системы.

Обстановка изменяется с использованием преступником специальных средств совершения преступления, таковыми являются программные, аппаратно-программные средства, а также с наличием или отсутствием средств защиты компьютерной информации.

В результате киберпреступления в обстановке могут оставаться характерные изменения – электронно-цифровые следы. Однако они обладают спецификой, которая проявляется в том, что многие изменения остаются практически незаметными.

Киберпреступлениям во многом способствует низкая информационная безопасность, не только частная, и корпоративная. Еще один фактор отмеченный В.В. Поляковым «косвенным образом способствует

---

[27] Агибалов А.Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. … канд. юрид. наук. Воронеж, 2010. С. 21.

[28] Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы : монография. Омск, 2009. С. 243 – 246.

противоправной деятельности преступников … недостаточный уровень квалификации правоохранительных органов в области расследования преступлений в сфере высоких информационных технологий»[29].

Обстановка преступлений в сфере компьютерной информации несет в себе большую информационную базу. Знание о ней, ее особенностей и влияния на преступления представляются важными для составления криминалистической характеристики киберпреступлений.

2.3 Личность преступника

Научно-технический прогресс как социальное явление породил появление новых правоотношений между людьми. Следствием прогресса также является и негативная тенденция роста преступности, связанной непосредственно с нарушением законодательства в сфере компьютерной информации.

Специалисты, ведущие расследование преступных деяний, на практике сталкиваются с рядом проблем, обусловленных спецификой данного вида преступления в виду того, что средства и методы, применяемые относительно данной категории, еще недостаточно разработаны, что является допущением криминалистической науки. Для устранения данной проблемы «в криминалистической литературе уделяется повышенное внимание методике расследования компьютерных преступлений, в этой области еще остается ряд нерешенных и дискуссионных вопросов. В частности, нуждается в уточнении криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации»[30].

---

[29] Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АГУ. 2013. № 2-1 (78). С. 114 – 116.

[30] Головин А.Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации // Электрон. дан. – 2018. – URL: http://www.crime-research.org/library/Golovin.htm (дата обращения: 07.01.2018 г.)

Криминалистическая характеристика лиц, совершающих компьютерные преступления, подкрепленная результатами эмпирических исследований, может быть положены в основу концепции предупреждения и профилактики преступлений в сфере компьютерной информации, использована при разработке криминалистических методик их расследования, применена в процессе расследования конкретных компьютерных преступлений.

К криминалистической характеристике личности преступника как составной части криминалистической характеристики киберпреступлений в целом можно отнести сведения о социальных, социально-демографических, социально-психологических свойствах личности преступника, то есть сведения о его поле, возрасте, состоянии гражданства, полученном образовании, социальном и должностном положении лица, прежних судимостях, его характере, мотивах и целях совершения преступления, роли в преступлении и других признаках личности преступника.

В криминалистической науке существует множество классификаций лиц, совершающих преступления в сфере компьютерной информации.

Наиболее интересной, по нашему мнению, является классификация А.В. Кузнецова, согласно которой данных преступников можно разделить на три категории:

- к первой группе относятся лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма, и изобретательности, они воспринимают средства компьютерной техники как вызов их творческим и профессиональным знаниям, умениям и навыкам;

- вторая группа включает лиц, страдающих новым видом психических заболеваний – информационными или компьютерными фобиями;

- в третью группу входят профессиональные «компьютерные» преступники с ярко выраженными корыстными мотивами.

Данная группа, по мнению указанного автора, представляет собой наибольшую угрозу для общества[31]. Из этого следует сделать вывод, что субъектом преступления не обязательно должен быть высококвалифицированный специалист с большим стажем работы в сфере информационных технологий, на самом деле в зависимости от цели им может быть абсолютно любой человек, обладающий базовыми знаниями.

В данной категории преступлений целью в основном являются корыстные побуждения, выражающиеся в краже, реализации похищенного программного обеспечения, получение охраняемой законом информации и передача ее третьим лицам за определенное вознаграждение, неправомерный доступ к бесплатным каналам связи, совершение экономических преступлений посредством информационных технологий. Отдельное внимание стоит уделить преступлениям, совершаемым из хулиганских побуждений, не имеющих целью личный интерес, а лишь нанесение вреда какому-либо лицу[32].

Касательно возраста преступника, следует отметить, что в основном поданной категории дел виновными являются молодые люди до 30 лет.

Г.Т. Мегрелишвили делит киберпреступников на несколько групп:

1. К первой группе автор относит лиц, отличительной особенностью которых является сочетание профессионализма и фанатизма в области компьютерной техники и программирования. Такие лица не имеют четкого противоправного намерения, действуют исключительно для проявления своих профессиональных и интеллектуальных способностей. Они любознательны и азартны. Повышение мер по обеспечению компьютерной безопасности рассматривают как вызов их способностям.

Особенности совершения киберпреступления данной группой лиц выражаются в отсутствии подготовки и плана действий, оригинальности

[31] Кузнецов А. В. Некоторые вопросы расследования преступлений в сфере компьютерной информации // Информационный бюллетень следственного комитета МВД РФ. М., 1998. № 2. С. 42-48.

[32] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия-Телеком, 2002. С. 161.

способа совершения, а также в том, что меры по сокрытию преступления не принимаются.

2. Во вторую группу входят лица, страдающие информационными заболеваниями или компьютерными фобиями – это новым видом психических расстройств, тем не менее, признанных Всемирной организацией здравоохранения.

Киберпреступления, совершаемые этими лицами, чаще всего связаны с уничтожением компьютерных данных.

3. Третью группу лиц – являются высококвалифицированными специалистами, чаще всего имеющими высшее техническое образование. Однако, в отличие от первой группы, это профессионалы с устойчивыми преступными навыками и ярко выраженными корыстными целями. Совершают киберпреступления многократно и принимают меры по сокрытию своих действий[33].

В своей статье «Общая характеристика психологии киберпреступника» А.Н. Косенковым и Г.А. Черным в зависимости от мотивации выделены следующие типы киберпреступников.

Корыстный тип. Помимо характерных для обыкновенного корыстного типа преступников свойств, киберпреступники могут совершать преступления для получения специфических предметов, имеющих особую ценность в киберпространстве, например, хищение игровых предметов, учетных записей игроков, игровой валюты и иных предметов, без цели их дальнейшей продажи.

Насильственный тип. Несмотря на отсутствие физического контакта, такие насильственные преступления, как доведение до самоубийства или угроза убийством, могут быть совершены при помощи электронных устройств и сетей.

---

[33] Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий // Вестник Том. гос. ун-та. 2007. № 299. С. 180 - 181

Сексуальный тип. Наиболее распространенная деятельность – незаконное распространение порнографических материалов или предметов, понуждение к действиям сексуального характера, развратные действия.

Социально-дезорганизующий тип. Основная цель – нарушение законодательно закрепленных социальных норм, разрушительное влияние на общественные отношения.

Идеологически или политически мотивированный тип, совершающий преступления по политическим или идеологическим убеждениям.

Статусный тип. Преступники этого типа, совершая преступления, стремятся получить высокий неформальный социальный статус. В среде киберпреступников статусность может иметь важное значение как мотив.

Исследовательский тип. Основой мотиваций данного типа является изучение программных и аппаратных составляющих электронных устройств и их сетей, поиск уязвимостей, возможности их использования и устранения[34].

Согласно исследованию Орли Тургеман–Голдшмита, лектора израильского университета, свою деятельность и цели киберпреступники истолковывают по-разному. Все они характеризуют себя как положительные и экстраординарные личности, которые являются носителями социальных изменений и демонстрируют лучшее поведение. Главным выводом исследования является то, что вины за свои преступные действия киберпреступники не ощущают[35].

Н.Н Федотовым также описаны несколько типичных образов киберпреступников.

1. «Хакер» (условное наименование). Основными мотивами данного типа являются исследовательский интерес, честолюбие, желание показать свои возможности. Наличие сложных средств защиты компьютерных систем

[34] Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Криминологический журнал БГУЭП. 2012. № 3 (21). С.87 - 94

[35] Orly Turgeman–Goldschmidt. Meanings that Hackers Assign to their Being a Hacker [Электронный ресурс] // Электрон. дан. – 2017. – URL: http://www.cybercrimejournal.com/Orlyijccdec2008.pdf (дата обращения 03.02.18).

и компьютерных данных воспринимаются хакерами как вызов своим способностям.

Казалось бы, что к подобному типу преступников должны относиться пользователи с высоким уровнем знаний в области IT. Однако практика показывает, что основная часть хакеров имеет средний уровень знаний. Можно предположить, что успехов в своей деятельности среднестатистический хакер достиг, получив конкретные знания в Сети – в настоящее время популярно выкладывать в Интернет различные инструкции (так называемые «гайды»).

2. «Инсайдер» (условное наименование). По мнению Н.Н. Федотова является наиболее распространенным типом киберпреступника, с невысоком уровнем знаний в области IT. Его отличительная особенность заключается в том, что в силу служебного положения он обладает доступом в информационную систему. Согласно статистике, большая «взломов» производится сотрудниками, то есть изнутри.

3. «Белый воротничок» (условное наименование). Данный тип представляется как заядлый казнокрад, для которого компьютерные системы стали новым инструментом преступной деятельности. Наиболее распространенными преступлениями, совершаемыми данным типом киберпреступника являются хищение средств, взяточничество, коммерческий подкуп и продажа информации, которая может составлять коммерческую тайну и так далее.

Среди «белых воротничков» могут выделяться личности, злоупотребляющие своим служебным положением из–за обиды на начальство или компанию и т.п., а также расхитители с полным отсутствием моральным принципов, которые занимаются данной преступной деятельностью только потому, что у них имеется такая возможность. Также Н.Н. Федотов выделяет и тех, кто попал в тяжелое материальное положение[36].

[36] Федотов Н.Н. Форензика – компьютерная криминалистика. М., 2007. С. 45.

4. «Е–бизнесмен» (условное наименование). Как правило, не является квалифицированным специалистом в области IT и не имеет служебного положения, которым может злоупотребить. Решение о совершении правонарушения принимается исключительно ради выгоды.

Выгодность киберпреступления в большинстве случаев связана со сложностью организации или технического обеспечения. Эти элементы влияют на успешность компьютерного преступления. Поэтому чаще всего «е–бизнесмены» отличаются хорошими способностями к предпринимательству и организации.

Данный тип преступников обычно занимается кардингом и фишингом.

5. «Антисоциальный тип» (условное наименование). В данном случае мотивом киберпреступника является социопатия, то есть патологическая тяга к подобного рода деятельности. Такие личности действуют импульсивно, так как не способны к предварительному планированию.

Мы считаем верным утверждение, что причиной девиантного поведения компьютерных пользователей является влияние, которое оказывает на их сознание киберпространство. Данная теория была предложена профессором Джоном Сулером (США). Им было введено понятие «эффект онлайн дезингибиции» [37] . Сущность данного эффекта заключается в том, что в условиях анонимности в киберпространстве люди отделяют свои действия и свою реальную личность, полагая, что может не брать на себя ответственность за свои действия, совершенные в киберпространстве.

Применение юридической психологии при расследовании компьютерных преступлений необходимо в силу отсутствия достаточного количества материальных следов преступника, разнообразия возможных мотивов киберпреступников, невозможность установления определенного

[37] John Suler. The Psychology of Cyberspace [Электронный ресурс] // Электрон. дан. – 2017. – URL: http://users.rider.edu/~suler/ psycyber/psycyber. (дата обращения 30.11.2017).

круга лиц, которые могли совершить преступление, а также потенциально большой вред, который может нанести киберпреступление.

Криминалистическая характеристика лиц, совершающих компьютерные преступления, подкрепленная результатами эмпирических исследований, может быть положены в основу концепции предупреждения и профилактики преступлений в сфере компьютерной информации, использована при разработке криминалистических методик их расследования, применена в процессе расследования конкретных компьютерных преступлений.

ГЛАВА 3 Использование криминалистической характеристики при расследовании преступлений в сфере компьютерной информации

Говоря о расследовании преступлений в сфере компьютерной информации следует подчеркнуть, что расследование преступлений в сфере компьютерной информации, особенности отдельных следственных действий приобрели в последнее время особую актуальность, в связи с большим количеством преступлений, совершенных в данной сфере.

Ввиду довольно высокого уровня латентности исследуемого вида преступлений большое значение приобретает деятельность правоохранительных органов по их выявлению.

В сфере компьютерной информации преступления раскрываются достаточно сложно, так как нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место (например, сбой в работе ЭВМ и программного обеспечения, средств электросвязи, энергообеспечивающего оборудования; замыкания в электропроводке и т.п.).

Одной из особенностей в расследовании данной категории преступлений, является привлечение специалиста, четко знающего свои задачи, права и обязанности, для оказания помощи следователю.

Основные криминалистические особенности компьютерной информации заключаются в следующем:

1) она достаточно просто и быстро преобразуется из одной объектной формы в другую, копируется (размножается) на различные виды машинных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств электросвязи;

2) при изъятии компьютерной информации, в отличие от изъятия материального предмета (вещи), она сохраняется в первоисточнике, т.к. доступ к ней могут одновременно иметь несколько лиц, например, при

работе с информацией, содержащейся в одном файле, доступ к которому одновременно имеют несколько пользователей сети ЭВМ.

Алгоритм расследования преступлений в сфере компьютерной информации складывается в зависимости от состава совершенного преступления и исходной следственной ситуации[38].

Основанием для возбуждения уголовного дела, как правило, служат заявления потерпевших – законных пользователей, работающих в сети на основании договора с фирмой-провайдером[39].

При расследовании преступлений в сфере компьютерной информации можно выделить (как и по другим категориям) три типичные следственные ситуации. Преступление, связанное с движением компьютерной информации, произошло:

– в условиях очевидности – характер и его обстоятельства известны (например, какой вирус и каким способом введен в компьютерную сеть) и выявлены потерпевшим собственными силами, преступник известен и задержан (явился с повинной);

– известен способ совершения, но механизм преступления в полном объеме неясен, например, произошел несанкционированный доступ к файлам законного пользователя через Интернет, через слабые места в защите компьютерной системы, преступник известен, но скрылся;

– известен только преступный результат, например, дезорганизация компьютерной сети банка, механизм преступления и преступник неизвестны.

В первом случае необходимо установить, имелась ли причинно-следственная связь между несанкционированным проникновением в компьютерную систему и наступившими последствиями (сбоями в работе, занесением компьютерного вируса и пр.), определить размеры ущерба, провести личный обыск, допрос задержанного, свидетелей, осмотр места

---

[38] Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. М., 2001. С. 65.

[39] Вехов Б. В. Компьютерные преступления. Способы совершения. Методики расследования. М., 1996. С. 48.

происшествия с участием соответствующих заранее приглашенных специалистов и т.д.). Во втором и третьем – первоочередной задачей, наряду с указанными выше, является розыск и задержание преступника, получение объяснения (допрос) заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей (очевидцев), вызов и инструктаж необходимых специалистов для участия в осмотре места происшествия, осмотр места происшествия (с осмотром, предварительным исследованием и изъятием машинных носителей и компьютерной информации, средств вычислительной техники, документов и т.п.), проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, определения рабочего места преступника, обнаружения следов и других вещественных доказательств и т.д.

Кроме того, имеются и определенные трудности получения и использования в процессе доказывания результатов производства технико-криминалистической экспертизы компьютерных систем. Производство экспертизы компьютерной техники и, соответственно, получение заключения эксперта предоставляет в распоряжение как следователя, так и, в дальнейшем, суда достаточно веские доказательства, подтверждающие или, наоборот, опровергающие виновность лица, привлеченного к уголовной ответственности.

Как верно указывают Э.В. Лядов и Т.А. Сулейманов, не смотря на кажущуюся простоту, при назначении технико-криминалистической экспертизы компьютерных систем следователи сталкиваются с некоторыми серьезными проблемами.

Во-первых, это отсутствие в штате экспертных подразделений правоохранительных органов и Министерства юстиции высококвалифицированных специалистов в области компьютерной информации.

Во-вторых, отсутствие у большинства следователей достаточной подготовки для формирования четких и правильно сформулированных вопросов эксперту (не выходящих при этом за рамки его специальных познаний) при назначении вышеуказанных экспертиз.

В-третьих, определенные трудности, связанные со второй обозначенной проблемой, при интерпретации заключений экспертов, правильного их понимания и уяснения хода проводимых исследований при производстве экспертизы[40].

В заключение следует отметить, что способы совершения компьютерных преступлений в настоящее время отличаются значительным и постоянно расширяющимся разнообразием. Совершают преступления данной категории чаще всего лица со специальной подготовкой в области автоматизированной обработки информации, причем более половины из их числа в составе преступных групп. Основная опасность исходит от внутренних пользователей – ими совершается более 90% преступлений.

При производстве предварительного расследования по делам о преступлениях в сфере компьютерной информации особую сложность вызывает осуществление следственных действий, связанных с обнаружением и сбором вещественных доказательств: осмотр, обыск и выемка.

Необходимо по возможности детально изучить обстановку места проведения следственного действия: определить расположение и планировку помещения и выяснить режим доступа в помещение.

Также целесообразно определить, какие действующие средства компьютерной техники находятся в помещении и как они взаимосвязаны друг с другом и с сетями общего пользования; установить действующие средства защиты информации.

[40] Лядов Э.В., Сулейманов Т.А. К вопросу о некоторых проблемах производства технико-криминалистической экспертизы компьютерных систем // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 279 - 282.

Важным фактором является участие специалиста в области информационных технологий. С его помощью нужно подготовить специальные технические и программные средства, которые могут быть полезны во время производства обыска, осмотра или выемки, провести инструктаж лиц, участвующих в следственном действии, определить наиболее оптимальное время его производства.

На основном этапе проведения следственных действий при производстве по делам о преступлениях в сфере компьютерной информации особое внимание необходимо уделить следующим моментам.

При прибытии следственной группы на место производства следственного действия значимым является решение вопроса о целесообразности отключения энергопитания. При этом следователь должен учитывать, что, с одной стороны, предварительное отключение энергии позволит предотвратить действия злоумышленников, направленные на сокрытие следов преступления при помощи средств компьютерной техники (как удаление компьютерной информации, так и уничтожение информации на бумажных носителях при помощи шредера), но с другой – принудительное отключение уничтожит информацию, хранящуюся в оперативном запоминающем устройстве электронно-вычислительной машины, которая может быть полезна для расследования преступления. Кроме того, эта мера может не возыметь должного результата вследствие использования владельцем средств компьютерной техники источников бесперебойного питания.

Сразу после прибытия на место производства следственных действий необходимо исключить возможность внесения изменений в компьютерную информацию. Следователь должен распорядиться, чтобы персонал покинул рабочие места без прекращения работы техники и без завершения программ. Лучший вариант здесь – «оставить все как есть». Нужно также установить охрану, наблюдение за рабочими местами, серверами, а также щитами управления энергопитанием.

Если место проведения следственного действия оборудовано спутниковой связью (как, например, многие таможенные посты), то следует установить контроль над устройством связи, чтобы предотвратить возможное умышленное нарушение его работы. Особое внимание стоит обратить на мобильные устройства удаленного доступа (например, «3G», «4G» модемы), а также необходимо отключить беспроводные устройства передачи данных (например, «Wi-Fi», «Bluetooth») при их наличии на исследуемых средствах компьютерной техники.

Далее важно как можно быстрее определить ЭВМ, на которой располагается компьютерная информация, представляющая наибольший интерес для целей расследования. После этого стоит установить периферийные устройства, сопряженные с интересующей следствие ЭВМ. Это целесообразно сделать для обнаружения информации, которую злоумышленник может хранить на этих устройствах, а также для выявления иных следов преступления.

Современные технологии позволяют хранить большие объемы информации на относительно малых по размеру носителях. В этой связи нужно предпринять действия, направленные на обнаружение носителей компьютерной информации (вплоть до личного обыска). На мобильных носителях может содержаться информация как являющаяся предметом компьютерного преступления (например, незаконно скопированная база данных), так и использовавшаяся в качестве средства совершения преступления (например, вредоносная программа, применявшаяся для преодоления программных средств защиты информации). Стоит обратить особое внимание на возможность наличия в системном блоке ЭВМ заранее преднамеренно отключенных жестких дисков [41] , которые не будут отображаться в системном каталоге при традиционном исследовании ЭВМ, но могут содержать важную информацию.

[41] Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной информации // Законность. 1999. № 3. С. 12 - 15.

В процессе расследования также не стоит недооценивать традиционные, «некомпьютерные» следы преступления. Так, например, исследование потожировых следов на устройствах ввода, носителях информации, других периферийных устройствах будет чрезвычайно полезно для установления лиц, причастных к совершению преступления в случаях, когда доступ в помещение с находящейся в нем ЭВМ, при помощи которой было совершено преступление, имеет большое число лиц. Помимо этого, информация, имеющая отношение к преступлению, может быть распечатана злоумышленником (например, код вредоносной программы) или сохранена любым другим (неэлектронным) способом (например, пароль доступа к защищенной информации может быть записан на бумажном носителе; использование пароля значительно ускорит процесс исследования ЭВМ при нежелании подозреваемого сотрудничать с правоохранительными органами).

Применение перечисленных выше мер характерно для всех случаев проведения указанных следственных действий. Однако в случае необходимости производства обыска, осмотра или выемки средств компьютерной техники, принадлежащей таможенным органам, следователь также должен учитывать и другие факторы.

Уже на первоначальном этапе следственного действия должно быть достоверно известно, какие средства компьютерной техники находятся в помещении, в котором проводится следственное действие, какое программное обеспечение используется, где находятся серверы, какова система энергоснабжения, кто является ответственным лицом и т. д. Получение такой информации возможно путем истребования у вышестоящего таможенного органа необходимой должностной документации, в которой указаны необходимые сведения. Вместе с тем следователем должны быть приняты меры по обеспечению внезапности проведения обыска. Кроме этого, целесообразным может оказаться поручение оперативным сотрудникам собрать негласными методами необходимую информацию.

Таким образом, первоначальный этап характеризуется возможностью получения большего объема информации об обстановке места проведения следственного действия, что позволяет качественно подготовиться к основному этапу.

Положительное решение вопроса об отключении электроэнергии перед производством следственного действия нецелесообразно, так как в таможенных органах источниками бесперебойного питания оснащены практически все АРМ.

При производстве обыска или осмотра внезапное появление следственной группы будет значительно затруднено тем фактом, что таможенные органы располагаются на охраняемых территориях. Поэтому следователь должен предпринять меры, направленные на сохранение внезапности.

Также необходимо учитывать характер данных, обрабатываемых таможенными органами, – большая часть является информацией ограниченного доступа (в том числе и составляющая государственную тайну). Таким образом, следователем должны быть предприняты меры по обеспечению защиты такой информации во время производства следственного действия.

На сегодняшний день информационные системы таможенных органов России характеризуются высоким уровнем взаимосвязанности их элементов. Большинство АРМ, используемых таможенными органами, объединены в Ведомственную интегрированную телекоммуникационную сеть, что значительно затрудняет поиск следов преступления из-за увеличения количества ЭВМ, которые необходимо исследовать.

Поскольку в таможенных органах используются технические и программные средства защиты информации, преодоление которых является очень сложным процессом, первоочередное внимание необходимо уделить сотрудникам и работникам таможенного органа, так называемым «инсайдерам». На службу в таможенные органы принимают граждан РФ с

высшим образованием (в том числе и техническим), следовательно, при производстве обыска или осмотра прежде всего необходимо исследовать АРМ должностных лиц, имеющих техническое образование, так как вероятность того, что они обладают специальными познаниями, необходимыми для совершения преступления в сфере компьютерной информации, выше, чем у остальных сотрудников.

Производство таких следственных действий, как обыск, выемка и осмотр, в таможенных органах по делам о преступлениях в сфере компьютерной информации указанные выше особенности, которые необходимо учитывать для достижения наилучших результатов.

ГЛАВА 4 Актуальные проблемы выявления и раскрытия преступлений в сфере компьютерной информации

В наши дни жертвами преступлений в сфере информационных технологий становятся не только руководители высшего звена и правительственные организации, но и простые граждане. «При этом безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников»[42].

Количество преступлений, совершаемых в сфере компьютерной информации и высоких технологий увеличивается соразмерно росту пользователей компьютерных сетей. Об этом в частности свидетельствуют отдельные электронные ресурсы, разработанные правительствами некоторых стран мира для приема заявлений граждан на преступления, совершенные в телекоммуникационной сети «Интернет».

Так запущенный в мае2000 года как виртуальный центр для приема жалоб граждан США на «интернет-преступления» сайт «InternetComplain Center» получил своего миллионного заявителя спустя семь лет после создания (июнь 2007 года). В ноябре 2010 года было зарегистрировано два миллиона жалоб на «интернет-преступления». В 2014 году количество заявлений достигло трёх миллионов. Ежегодно, начиная с 2010 года количество заявлений граждан США на совершенные в отношении них в телекоммуникационной сети «Интернет» преступления приближается к отметке в 300 тысяч (2010 – 303,809; 2011 – 314,246; 2012 – 289,974; 2013 – 262,813; 2014 – 269,422; 2015 – 288,012). По сообщениям интернет-пользователей общие потери от киберпреступности за 2015 год составили 1,070,711,522 доллара США[43].

---

[42] Номоконов, В.А. Киберпреступность как новая криминальная угроза /В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. Санкт-Петербург. 2012. № 1 (24). С. 45.

[43] Центр интернет-мониторинга жалоб на преступления в электронной сети [Электронный ресурс] // Официальный сайт ФБР США. – Электрон. дан. – 2018. – URL: //www.ic3.gov (дата обращения: 01.02.2018).

В России подобные электронные ресурсы пока не введены в действие, а официальная статистика сообщает о не значительном количестве киберпреступлений.

Так по данным отчета о состоянии преступности, ежегодно размещаемого на сайте Министерства внутренних дел, в России за 2016 год было зарегистрировано 1748 преступлений в сфере компьютерной информации, что на 26,6 % меньше чем за аналогичный период в 2015 году. 1503 преступления было выявлено сотрудниками ОВД. Из преступлений, дела и материалы о которых находились в производстве, было раскрыто 903 деяния[44].

По сравнению с официальной статистикой в США и некоторых странах Западной Европы приведенные цифры кажутся ничтожными. Даже если принять во внимание противоправные деяния, которые при использовании компьютерной информации и высоких технологий (способ совершения деяния) несомненно, относятся к киберпреступлений и размещены в разных главах особенной части УК РФ.

В частности, «Нарушение неприкосновенности частной жизни» (ст. 137 УК РФ), «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» (ст. 138 УК РФ), «Мошенничество в сфере компьютерной информации» (ст. 159.6 УК РФ), «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» (ст. 183 УК РФ),

«Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних» (ст. 242.1 УК РФ), «Незаконные изготовление и оборот порнографических материалов или предметов (ст. 242 УК РФ).

В связи с этим возникает вполне логичный вопрос о фактическом состоянии (количестве и качестве) совершаемых в Российской Федерации

[44] Официальный сайт МВД РФ [Электронный ресурс] // Электрон. дан. – 2018. – URL: //www.мвд.рф (дата обращения: 15.02.2018).

преступлений в сфере компьютерной информации и высоких технологий, об их официальной государственной регистрации и латентном характере деяний в указанной сфере.

Отдельно – вопрос об уровне профессиональной подготовленности сотрудников правоохранительных органов, социализирующихся на выявлении, раскрытии и расследовании названных преступлений.

Проведённый опрос оперативных сотрудников и следователей, работающих на территории г. Рязани и Рязанской области показал, что ключевой проблемой в сфере киберпреступлении являются недостаточная «техническая подкованность» названных сотрудников.

Так, 97,5 % респондентов имеют высшее юридическое образование, и только 5 % (4 человека) получили второе техническое образование по следующим специальностям: 02.00.00 – компьютерные и информационные науки, 09.00.00 – информатика и вычислительная техника, 11.00.00 – электроника, радиотехника и системы связи.

Опрос вышеуказанных респондентов на предмет определения уровня владения компьютерной техникой и современными электронными устройствами также подтвердил тот факт, что киберпреступники по-прежнему технически грамотнее сотрудников полиции (юстиции). 72 % опрошенных респондентов оценили свои знания в этой области на уровне «среднего пользователя», способного самостоятельно использовать электронно-вычислительные машины для решения повседневных задач, связанных с набором текста, выходом в Интернет и другими не сложными манипуляциями с компьютерной техникой. 23 % опрошенных лиц оценили свои знания на уровне «продвинутого пользователя», способного самостоятельно переустановить операционную систему, поставить защиту от вредоносных программ, поменять формат используемых файлов, восстановить утраченную информацию и т.д. 5 % опрошенных респондентов, имеющих техническое образование оценили свои знания компьютерной техники как «высокие». В то же время как показало исследование, даже они

не всегда обладают достаточными знаниями и практическим опытом для выявления и раскрытия преступлений в сфере компьютерной информации и высоких технологий. Например, определить IP – адрес (уникальный сетевой адрес узла в компьютерной сети, построенный по протоколу IP) лица, который можно передать провайдеру с целью установления местонахождения (адреса проживания) пользователя услуг интернета – преступника.

Как следствие появление другой проблемы, связанной с несвоевременностью выявления и раскрытия киберпреступлений. Так по опросам респондентов было установлено, что в 49 % случаев с момента реализации преступного умысла в сети Интернет и до поступления в полицию информации о совершенном преступлении проходит свыше 10 суток. 79 % респондентов отметили, что в 84 % случаев срок проверки сообщения о совершении преступления в сфере компьютерной информации и высоких технологий продлевается до 10 и 30 суток, в том числе по причине отсутствия на местном (районном) уровне специалистов способных правильно оценить событие преступления.

Как следствие 74 % опрошенных респондентов отметили факт несвоевременного (запоздалого) начала предварительного расследования, когда значительная часть важных доказательств была утрачена, в том числе по вине потерпевшего, пытавшегося самостоятельно решить сложившуюся ситуацию.

При попытке выяснить у респондентов (преимущественно следователей) тактику и методику, которую бы они избрали в рамках расследования наиболее распространенных киберпреступлений, последние называли такие стандартные следственные действия как осмотр места происшествия, обыск по месту жительства, изъятие компьютерного оборудования, назначение по нему экспертиз технического профиля, допрос подозреваемого и т.д. В то же время у 82 % респондентов возникли трудности, связанные с определением конкретного места происшествия.

Например, в рамках расследования телефонного мошенничества связанного с использованием услуги «мобильный банк» или мошенничества с пластиковыми картами. 78 % опрошенных лиц не смогли четко сформулировать вопросы, которые бы они поставили на разрешение эксперту в рамках компьютерно-технической экспертизы[45, 46]. 66 % респондентов посчитали, что затратили бы значительно больше времени на подготовку плана допроса лица, подозреваемого в совершении киберпреступления. В том числе в рамках предварительных консультаций со специалистами в сфере компьютерных технологий.

Подводя итог вышесказанному можно сделать вывод о том, что выявление, раскрытие и расследование преступлений в сфере компьютерной информации и высоких технологий, по-прежнему остается одной из труднейших задач для уголовного розыска и органов предварительного расследования. Это, безусловно связано с целым рядом проблем, среди которых выделяются такие из них как отсутствие должного мониторинга следственной и судебной практики в области киберпреступлений, в целом не значительным опытом работы, подготовкой следователей и сотрудников уголовного розыска, которые ранее не сталкивались с подобными преступлениями, наконец, общая нехватка научно обоснованных и апробированных на практике методических рекомендаций по тактике и методике расследования преступлений в сфере компьютерной информации и высоких технологий.

[45] Огородников С.Н. Судебные экспертизы и типичные ошибки при их назначении (проведении) // Актуальные проблемы уголовного процесса и криминалистики. Рязань, 2016. С. 203 – 206.

[46] Пинчук Л.В. К вопросу о следственных ошибках, допускаемых при назначении экспертиз // Актуальные проблемы уголовного процесса и криминалистики. Рязань, 2016. С. 279 – 283.

ЗАКЛЮЧЕНИЕ

Мы живем в эпоху информационного общества, и наша жизнь тесно связана с различными технологиями и сетью Интернет. И практически каждый раз, взаимодействуя с компьютерными технологиями, мы подвергаем себя угрозе стать жертвой киберпреступников. Потому всестороннее изучение компьютерных преступлений позволит разработать эффективные меры по их предупреждению и расследованию

Диссертационное исследование выполнено с целью разработки на основе анализа теоретических положений и изучения правоприменительной практики научно обоснованных рекомендаций, направленных на совершенствование криминалистической деятельности, осуществляемой при расследовании преступлений в сфере компьютерной информации.

Подводя итог проведенного исследования, обозначим некоторые положения из целого ряда выводов, на которых обосновывается данная работа.

1) Изучая различные подходы к определению понятий «киберпреступность» и «компьютерные преступления», мы согласились с мнением большинства исследователей, это преступность, связанная как с использованием компьютеров или компьютерных данных, так и информационных технологий и глобальных сетей, а также специального программного обеспечения. Потому понятия «киберпреступность» и «компьютерные преступления» в данной работе отождествлены.

2) В настоящее время в числе компьютерных преступлений преобладают: мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ) нарушение авторских и смежных прав, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст.

273 УК РФ); кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ).

3) Ввиду довольно высокого уровня латентности исследуемого вида преступлений большое значение приобретает деятельность правоохранительных органов по их выявлению.

Говоря о расследовании данной категории дел, следует подчеркнуть, что расследование преступлений в сфере компьютерной информации, особенности отдельных следственных действий приобрели в последнее время особую актуальность, в связи с большим количеством преступлений, совершенных в данной сфере.

4) Киберпреступления можно охарактеризовать следующими признаками, которые создают существенные трудности при расследовании:

- высокий уровень профессиональной подготовки и технической оснащенности преступников;

- трансграничность совершения преступления;

- постоянное совершенствование способов совершения преступлений;

- высокоорганизованность преступников и др.

5) Борьба с киберпреступлениями, которые являются серьезной угрозой для личности и государства на фоне происходящих в мире изменений, как одна из задач правоохранительных органов, выдвигается на приоритетные позиции. Однако уже само выявление киберпреступления на данный момент представляет проблему, потому прослеживается высокая латентность преступлений в сфере IT.

В нашей стране отсутствует единая программа борьбы с киберпреступлениями. Для большинства сотрудников органов предварительного расследования раскрытие и расследование киберпреступлений представляет сложность, которая связана с тем, что при сборе доказательств и доказывании в таких делах необходимо изучение «виртуального следа». При этом уровень специальной технической подготовки, которая нужна для расследования подобных дел в органах

юстиции очень низкий. К тому же отсутствует обобщенный материал следственной практики, методический материал и рекомендации по расследованию данного вида преступлений.

Таким образом, научно-технический прогресс принес человечеству такие незаменимые в современной жизни новшества, как компьютеры и Интернет. Внедрение современных технологий повлекло за собой возникновение новых видов ресурсов - информационных. Но новые технологии стимулировали возникновение и развитие и новых форм преступности, в первую очередь компьютерных. Основную часть в этой сфере совершается с помощью компьютерных сетей. В последние годы специалистами замечена тенденция стремительного роста компьютерных преступлений посредством глобальной компьютерной сети Интернет.

Эффективная работа экспертных подразделений и криминалистов возможна при условии разработки специальных тактик проведения следственных действий, систематизации методик расследования киберпреступлений, а также подготовки специализированного кадрового состава. Все это, в совокупности, будет способствовать раскрытию киберпреступлений, даст возможность получать доказательства для предъявления их в суде. Российским криминалистам еще предстоит детально изучить киберпространство, разработать эффективные тактические и методические подходы к выявлению и расследованию киберпреступлений, которые в условиях глобального масштабирования более чем актуальны.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Научные статьи:

1. В.А. Номоконов, Л.В. Тропина Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 1 (24). – С. 45 – 55.
2. Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь. – 2004. – № 7. – С. 21 – 27.
3. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. – 2007. – № 2. – С. 17 – 25.
4. Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний // Российская юстиция. – 2011. – № 2. – С. 14 – 15.
5. Гавло В.К. Обстановка преступления как структурный компонент криминалистической характеристики преступления // Проблемы совершенствования тактики и методики расследования преступлений : сб. науч. трудов. — Иркутск, 1980. – С. 49 – 55.
6. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. – 2016. – № 1 (35). – С. 22 – 25.
7. Журавленко Н.И., Шведова Л.Е. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. – 2015. – № 3 (53). – С. 66 – 70.
8. Илюшин Д. А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг «Интернет» // Вестник Муниципального института права и экономики (МИПЭ). Липецк: Изд-во НОУ «Интерлингва». – 2004. – № 1. – С. 77 – 86.

9. Карпец И.И., Ратинов А.Р. Правосознание как элемент правовой культуры // Правовая культура и вопросы правового воспитания : сборник научных трудов. – М., 1974. – С. 55–57.

10. Комиссаров В.И. Обыск с извлечением компьютерной информации // Законность. – 1999. – № 3. – С. 12 – 15.

11. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Криминологический журнал БГУЭП. – 2012. – № 3 (21). – С. 87 – 94

12. Кузнецов А. В. Некоторые вопросы расследования преступлений в сфере компьютерной информации // Информационный бюллетень следственного комитета МВД РФ. – 1998. – № 2. С. 42 – 48.

13. Лядов Э.В., Сулейманов Т.А. К вопросу о некоторых проблемах производства технико-криминалистической экспертизы компьютерных систем // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 4-2. – С. 279 – 282.

14. Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий // Вестник Том. гос. ун-та. – 2007. – № 299. – С. 180 – 181.

15. Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста: научный журнал. – 2013. – № 5 (10). – С. 265 – 270.

16. Морар И.О. Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия? // Российский следователь. – 2012. – № 12. – С. 37 – 41.

17. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков. – Воронеж: Изд-во Воронеж. гос. ун-та. – 2002. – С. 94 – 119.

18. Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Компьютерная преступность и кибертерроризм: сборник научных работ. – 2004. – № 1. – С. 77 – 110.

19. Номоконов В.А., Тропина Л.В. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 1 (24). – С. 45 – 55.

20. Огородников С.Н. Судебные экспертизы и типичные ошибки при их назначении (проведении) / С.Н. Огородников, А.А. Рудавин, А.Н. Куфтерин // Актуальные проблемы уголовного процесса и криминалистики: сборник научных трудов, посвященный 15-летию принятия Уголовно-процессуального кодекса Российской Федерации. – Рязань: Рязанский филиал Московского университета МВД России имени В.Я. Кикотя. – 2016.– С. 203 – 206.

21. Пинчук Л.В. К вопросу о следственных ошибках, допускаемых при назначении экспертиз /Л.В. Пинчук, Д.С. Федосов // Актуальные проблемы уголовного процесса и криминалистики: сборник научных трудов, посвященный 15-летию принятия Уголовно-процессуального кодекса Российской Федерации. – Рязань: Рязанский филиал Московского университета МВД России имени В.Я. Кикотя. – 2016. – С. 279 – 283.

22. Писарев Е. В. Информационное взаимодействие следователя с экспертом // Вектор науки ТГУ. – 2014. – № 3 (29). – С. 211 – 214.

23. Поляков В.В. Анализ факторов, затрудняющих расследование неправомерного удаленного доступа к компьютерной информации // Проблемы правовой и технической защиты информации: сб. науч. ст. – Барнаул: Изд-во Алт. ун-та. – 2008. – С. 17–24.

24. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АГУ. – 2013. – № 2-1 (78). – С. 114 – 116.

25. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады ТУСУРа. – 2014. – № 2 (32). – С. 162 – 166.

26. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. 2012. № 24. С. 43 – 46.

27. Чекунов И.Г. Современные киберугрозы. Уголовно–правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. – 2012. – С. 9 – 22.

28. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. – 2012. – № 2. – С. 37 - 44.

29. Шевченко Е.С., Михайлюченко Н.Н. Киберпространство как элемент обстановки совершения преступлений // Академический юридический журнал. – 2015. – № 2. – С. 52 – 59.

30. Яблоков Н.П. Следственные ситуации в методике расследования и их оценка // Вестник Моск. ун-та. - Сер. 11. Право. – 1983. – № 5. – С. 12 – 17.

Учебная литература и монографии

31. Батурин Ю.М. Проблемы компьютерного права / Ю.М. Батурин. – М. : Юрид. лит., 1991. – 272 с.

32. Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. – М.: Юрлитинформ, 2015. – 340 с.

33. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 1996. – 182 с.

34. Возгрин И.А. Введение в криминалистику: История, основы теории, библиография. – СПб.: Юрид. центр Пресс, 2003. – 475 с.

35. Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. – Томск: Изд-во Том. ун-та, 1985. – 333 с.

36. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. – М., 2001. – 88 с.

37. Дуленко В.А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учебное пособие. – Уфа, 2007. – 210 с.

38. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. — М.: Горячая линия-Телеком, 2002. – 336.

39. Курс криминалистики: в 3 т. – Т. 3. Криминалистическая методика: Методика расследования преступлений в сфере экономики, взяточничества и компьютерных преступлений / под ред. О.Н. Коршуновой, А.А. Степанова. – СПб.: Юрид. центр Пресс, 2004. – 573 с.

40. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М.: Новый Юрист, 1998. – 256 с.

41. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы : монография. — Омск, 2009. – 480 с.

42. Расследование неправомерного доступа к компьютерной информации / Под ред. Н.Г. Шурухнова. – М.: Издательство «Щит-М», 1999. – 185 с.

43. Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов – М. : Норма, 2010. – 210 с.

44. Россинская Е.Р. Судебная экспертиза в уголовном, гражданском и арбитражном процессе: Практическое пособие. – М.: Право и Закон, 1996 г. – 220 с.

45. Степнов Е.А. Информационная безопасность и защита информации: учебное пособие / Е.А. Степнов, И.К. Корнеев. – М.: Инфра-М, 2001. – 304 с.

46. Федотов Н.Н. Форензика – компьютерная криминалистика / Н.Н. Федотов. – М. : Юрид. мир, 2007. – 432 с.

47. Шурухнов Н.Г. Расследование неправомерного доступа к компьютерной информации: учебное пособие / Н.Г. Шурухнов. – М. : Московский ун-т МВД России, 2004. – 352 с.

48. Ярочкин В.И. Информационная безопасность / В.И. Ярочкин. – М.: Международные отношения, 2000. – 400 с.

Диссертации и авторефераты диссертаций:

49. Агибалов А.Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. … канд. юрид. наук. – Воронеж, 2010. – 24 с.

50. Вехов В.Б. Криминалистическая характеристика компьютерных преступлений : автореф. дис. … канд. юрид. наук / Б.В. Вехов. – Волгоград, 1995. – 27 с.

51. Егорышев А. С. Расследование и предупреждение неправомерного доступа к компьютерной информации: дис. … канд. юрид наук. – Уфа, 2004. – 230 с.

52. Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дис. … канд. юрид. наук / Д.А. Илюшин. – Волгоград, 2008. – 233 с.

53. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет : автореф. дис. ... канд. юрид. наук. – Саратов, 2011. – 25 с.

54. Остроушко А. В. Организационные аспекты методики расследования преступлений в сфере компьютерной информации: дис. … канд. юрид. наук. – Волгоград, 2000. – 226 с.

55. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. … канд. юрид. наук. – Барнаул, 2009. – 238 с.

56. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. … канд. юрид. наук. – Барнаул, 2009. – С. 112 – 114.

57. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологические характеристики : дис. ... канд. юрид. наук. – Иркутск, 2006. – 237 с.

58. Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера: дис. … канд. юрид. наук. – Красноярск, 2010. – 206 с.

59. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. ... канд. юрид. наук. – Владивосток, 2005. – 25 с.

60. Шаталов А.С. Проблемы алгоритмизации расследования преступлений: автореф. дис. … д-ра юрид. наук. – М., 2000. – 35 с.

61. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : автореф. дисс. … канд. юрид. наук. – Москва, 2016. – 29 с.

62. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : дисс. … канд. юрид. наук. – Москва, 2016. – 249 с.

63. Шумилов Н.И. Криминалистические аспекты информационной безопасности: Дис. … канд. юрид. наук. – СПб.: Юрид. инст., 1997. – 164 с.

Нормативные акты и судебная практика:

64. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31. – Ст. 3451.

65. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31. – Ст. 3448.

66. Решение по делу 22-643/2018 (06.02.2018, Московский областной суд (Московская область))

67. Решение по делу 22-89/2018 (22-2921/2017;) (18.01.2018, Астраханский областной суд (Астраханская область))

68. Решение по делу 4/15-97/2017 (20.12.2017, Октябрьский районный суд г. Тамбова (Тамбовская область))

69. Решение по делу 2-3177/2017 ~ М-2576/2017 (14.12.2017, Минусинский городской суд (Красноярский край))

70. Решение по делу 2-3141/2017 ~ М-3294/2017 (14.12.2017, Норильский городской суд (Красноярский край))

71. Решение по делу 4/15-84/2017 (26.10.2017, Октябрьский районный суд г. Тамбова (Тамбовская область))

72. Решение по делу 22-897/2017 (25.10.2017, Верховный Суд Республики Марий Эл (Республика Марий Эл))

73. Решение по делу 1-73/2017 (25.10.2017, Уваровский районный суд (Тамбовская область))

74. Решение по делу 22К-6158/2017 (13.10.2017, Ставропольский краевой суд (Ставропольский край))

75. Решение по делу 1-488/2017 (11.10.2017, Кировский районный суд г. Томска (Томская область))

Электронные ресурсы:

76. Counsil of Europe. Convention on Cybercrime, Budapest. [Электронный ресурс] // Электрон. дан. – 2017. – URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/ (дата обращения 20.10.17).

77. John Suler. The Psychology of Cyberspace [Электронный ресурс] // Электрон. дан. – 2017. – URL: http://users.rider.edu/~suler/ psycyber/psycyber. (дата обращения 30.11.2017).

78. Orly Turgeman–Goldschmidt. Meanings that Hackers Assign to their Being a Hacker [Электронный ресурс] // Электрон. дан. – 2017. – URL: http://www.cybercrimejournal.com/Orlyijccdec2008.pdf (дата обращения 03.02.18).

79. Головин А.Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации // Электрон.

дан. – 2018. – URL: http://www.crime-research.org/library/Golovin.htm (дата обращения: 07.01.2018 г.)

80. Официальный сайт МВД РФ [Электронный ресурс] // Электрон. дан. – 2018. – URL: //www.мвд.рф (дата обращения: 15.02.2018).

81. Состояние преступности январь - декабрь 2017 года [Электронный ресурс] // Электрон. дан. – 2018. – URL: https://мвд.рф/reports/2/ (дата обращения: 11.02.2018).

82. Уголовный кодекс РФ [Электронный ресурс]: Федеральный закон от 13.06.1996 № 63-ФЗ принят ГД ФС РФ (с учетом всех поправок от 01.02.2018 г. № 139-ФЗ) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2018. – Доступ из локальной сети Науч. б-ки Том. гос. ун-та. (дата обращения 15.02.2018).

83. Центр интернет-мониторинга жалоб на преступления в электронной сети [Электронный ресурс] // Официальный сайт ФБР США. – Электрон. дан. – 2018. – URL: //www.ic3.gov (дата обращения: 01.02.2018).